(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Publication number: **0 363 122 A2**

# (12) EUROPEAN PATENT APPLICATION

(21) Application number: **89310051.1**

(51) Int. Cl.5: **G07F 7/10**

(22) Date of filing: **02.10.89**

(30) Priority: **03.10.88 JP 249561/88**

(43) Date of publication of application:
**11.04.90 Bulletin 90/15**

(84) Designated Contracting States:
**DE FR GB**

(71) Applicant: **FUJITSU LIMITED**
**1015, Kamikodanaka Nakahara-ku**
**Kawasaki-shi Kanagawa 211(JP)**

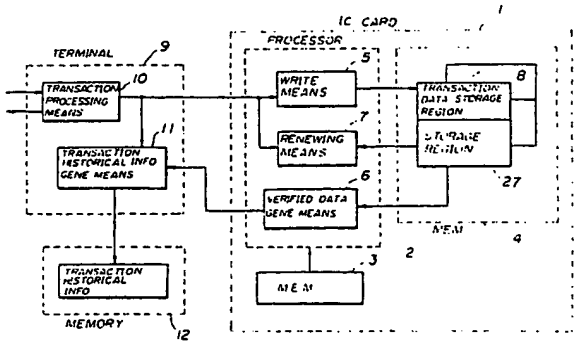
(72) Inventor: **Ogasawara, Nobuo**
**3-35-21-201, Nukuikitamachi**
**Koganei-shi Tokyo, 184(JP)**
Inventor: **Ozaki, Yoshiyuki**
**3-34-9, Nokendai Kanazawa-ku**
**Yokohama-shi Kanagawa, 236(JP)**

(74) Representative: **Stebbing, Timothy Charles et al**
**Haseltine Lake & Co. Hazlitt House 28**
**Southampton Buildings Chancery Lane**
**London WC2A 1AT(GB)**

## (54) Transaction authentication system.

(57) A transaction authentication system comprises a terminal (9, 20), a first memory (12, 18) and an IC card (1, 21, 51) which is detachably loaded into the terminal. The terminal supplies at least a transaction data which is related to a transaction and a designated storage region in a second memory (3, 4, 31, 32, 58, 59, 60) for storing the transaction data to the IC card when the IC card makes an access to a service via the terminal. A second processor (30, 54) of the IC card writes the transaction data received from the terminal in the designated storage region of the second memory and generates a verified data which is renewed every time the transaction data is written into the second memory. The verified data has a value in conformance with a predetermined generating algorithm and is stored in the second memory and also supplied to the terminal. A first processor (10, 11) of the terminal generates a transaction historical information which includes at least the designated storage region, the transaction data and the verified data and stores the transaction historical information in the first memory, so that a transaction is authenticatable from a correspondence of the verified data stored in the first memory and the verified data stored in the second memory.

FIG. 1




EP 0 363 122 A2

transaction being authenticatable from a correspondence of the verified data stored in the first memory means and the verified data stored in the second memory means. According to the transaction authentication system of the present invention, the verified data which is unique for each transaction is stored within the integrated circuit card and is also supplied to the terminal means to be stored in the first memory means. Hence, it is possible to authenticate the transaction by verifying the verified data stored within the integrated circuit card and the first memory means. The verified data cannot be fabricated or altered even by a person who is familiar with the programs of the terminal means, and the reliability of the integrated circuit card is greatly improved compared to the conventional case because illegal transactions can easily be found.

Other objects and further features of the present invention will be apparent from the following detailed description when read in conjunction with the accompanying drawings.

## BRIEF DESCRIPTION OF THE DRAWINGS

FIG.1 is a system block diagram for explaining an operating principle of a transaction authentication system according to the present invention;

FIG.2 is a system block diagram showing a first embodiment of the transaction authentication system according to the present invention;

FIG.3 is a system block diagram showing an embodiment of an IC card used in the first embodiment;

FIGS.4A and 48 respectively are a perspective view and a system block diagram for explaining the embodiment of the IC card shown in FIG.3 in more detail; and

FIG.5 is a system block diagram showing an embodiment of an IC card used in a second embodiment of the transaction authentication system according to the present invention;

FIGS.6A, 6B and 6C respectively are flow charts for explaining an operation of a central processing unit of the IC card shown in FIG.5; and

FIG.7 is a side view in cross section generally showing an embodiment of a card reader/writer which is used in the second embodiment.

## DESCRIPTION OF THE PREFERRED EMBODIMENTS

First, a description will be given of an operating principle of a transaction authentication system according to the present invention, by referring to FIG.1. The transaction authentication system generally comprises an IC card 1, a terminal 9, and a memory device 12. The IC card 1 comprises a processor 2, a first memory 3 which prestores a plurality of processing means (or programs) for operating the processor 2, and a second memory 4 which stores a transaction data which is processed by the operation of the processor 2. When making a transaction using the IC card 1, the transaction authentication system starts the transaction after authenticating a specific information which is stored in the IC card 1. The second memory 4 includes transaction data storage regions 8 which are respectively designated for each transaction and storage regions 27 which respectively store a transaction execution identifying information for each transaction in correspondence with a transaction data storage region 8. The processor 2 includes a write means 5 for designating the transaction data storage region 8 and for storing a transaction data therein, a verified data generating means 6 for generating a verified data for a transaction based on the transaction execution identifying information, and a renewing means 7 for renewing the transaction execution identifying information within the storage region 27 every time the transaction data is received.

The IC card 1 is loaded into the terminal 9 which can read and write information with respect to the IC card 1. The terminal 9 comprises a transaction processing means 10 for executing a transaction after the specific information of the IC card 1 is confirmed, and a transaction historical information generating means 11 for generating a transaction historical information in which a transaction data is added with a verified data which is read from the IC card 1 and an information which designates the transaction data storage region 8 for each transaction. The memory device 12 stores the transaction historical information which is received from the terminal 9.

The transaction is made as follows. That is, when the IC card 1 is loaded into the terminal 9, the terminal 9 reads a card identification information (for example, a card name) from the IC card 1 via a route which is not shown in FIG.1 and starts the transaction if the PIN can be confirmed. A transaction data which is obtained by the start of the transaction is output from the transaction processing means 10. The transaction data and an address data which designates a write address within the IC card 1 are supplied to the transaction historical information generating means 11 within the terminal 9 and the write means 7 and the renewing means 7 within the IC card 1.

The write means 5 writes the received transaction data at a designated address of the transaction data storage region 8 of the second memory 4. The renewing means 7 reads the transaction ex-

only the credit service, for example, the same card may be used for transactions with a plurality of stores and offices, accounts provided independently for each of the stores and offices, accounts in a plurality of banks and the like.

The IC card 21 is loaded into a card reader/writer (not shown) which is connected to the POS terminal 20. The card reader/writer reads from the IC card 21 the card identification information which identifies the IC card 21, and supplies the card identification information to a host computer (not shown). The host computer returns to the POS terminal a region designating information and the like for 20 designating a transaction data storage region 8 within the IC card 21.

Prior to making the transaction using the IC card 21, a check is made to prevent illegal use of the IC card 21. For example, a personal identification number (PIN) is entered by the user and the POS terminal 20 discriminates whether or not the entered PIN corresponds with a PIN which is prerecorded on the IC card 21, and the POS terminal 20 discriminates whether or not the use of the IC card 21 on the POS terminal 20 is permitted based on a terminal confirmation code.

Next, a description will be given of an operation of the first embodiment by referring to FIG.2. When the user uses the IC card 21 and purchases an item having a price of 200 dollars, for example, the operator of the POS terminal 20 loads the IC card 21 into the card reader/writer of the POS terminal 20 and enters the transaction sum of 200 dollars into the POS terminal 20. In this case, the transaction processing means 10 of the POS terminal 20 outputs a transaction sum data of 200 dollars and a transaction date data which includes the year, month and date of the transaction. The transaction processing means 10 further designates the storage region (area) where the transaction sum data and the transaction date data are to be stored. Based on the data received from the transaction processing means 10, the write means 5 of the IC card 21 writes the transaction data (transaction sum data and transaction date data) in a designated area A of the second memory 4. Then, the serial number generating means 25 of the IC card 21 generates the serial number. This serial number is stored in an internal memory and is supplied to the POS terminal 20.

The transaction historical information generating means 11 of the POS terminal 20 adds the serial number which is received from the IC card 21 to the transaction data (transaction sum data and transaction date data), the card identification information (for example, a card ID "CARD001") of the IC card 21, and the region designating information (area A in this case), so as to generate a unique transaction historical information among the plurality of IC cards, a plurality of POS terminals and a plurality of transaction data. The transaction historical information is written into the memory device 12 via a storing means 14. After the transaction ends, the transaction historical information is written into a memory device 18 within a host terminal 22 via communication means 15 and 16 and a storing means 17 by a batch data transmission.

The transaction is completed in the above described manner. When the transaction is legitimate, the serial numbers within the transaction historical information stored in the memory devices 12 and 18 change regularly in conformance with the generating algorithm. Hence, it is possible to authenticate the transaction by checking the change in the values of the serial numbers. When the transaction is legitimate, the serial number stored in the IC card 21 constantly corresponds with the serial number of the last transaction stored in the memory devices 12 and 18.

For example, the transaction historical information received from the POS terminal 20 may have been generated by an illegal user who not only knows the PIN but also knows the generating algorithm for the serial number. Such an illegal user can operate the POS terminal 20 and generate the transaction historical information without actually using the IC card 21. In this case, it is impossible to prohibit the illegal transaction itself, however, the serial numbers stored in the memory devices 12 and 18 after the transaction is made become different from the serial number stored in the IC card 21. Therefore, it is possible to find out that the illegal transaction has been made by verifying the serial number stored in the IC card 21 and the serial numbers stored in the memory devices 12 and 18, since the stored serial numbers do not correspond in the case of the illegal transaction.

In the first embodiment, the serial number is used as the verified data. However, it is possible to use a function as the verified data. In this case, the transaction execution identifying information x is taken as an argument and the verified data generating means 6 generates a function F(x). For example, the transaction execution identifying information x has an initial value $x_0$ and is renewed for every transaction such that the transaction execution identifying information x has a value $x_k$ when a kth transaction is made.

The function generated by the verified data generating means 6 need not necessarily be a single argument function and may be a multiple argument function. In the case of the multiple argument function, n arguments ($x_1$, $x_2$, $x_3$, ..., $x_n$) are renewed for every transaction.

The transaction execution identifying information for example has the initial value $x_0$ and values

step S12 sets a lock flag within the EEPROM 60 to an ON state and a locked state information is supplied to the terminal. When the lock flag is ON, the IC card 51 is made unusable for the selected service, and a locked state information is supplied to the terminal. In other words, the lock flag indicates whether or not the selected service is accessible by the IC card 51.

As described before, the IC card 51 may be used to receive various services. Hence, it is inconvenient if the IC card 51 were made unusable for all the services even when only predetermined one or more services should actually be made non-accessible. Therefore, in actual practice, the error number counter is provided for each service and the predetermined number used for the comparison in the step S11 is set for each service. In other words, a lock flag is provided for each service accessible by the IC card 51. For the sake of convenience, a description will hereunder be given of a case where only one lock flag is provided.

In FIG.6B, a transaction information write command including a transaction information and a write position within the IC card 51 is received from the terminal. A step S21 reads an authentication completion information, and a step S22 reads the lock flag. A step S23 discriminates whether or not the lock flag is ON. When the discrimination result in the step S23 is YES, a locked state information is supplied to the terminal. On the other hand, when the discrimination result in the step S23 is NO, a step S24 discriminates whether or not the authentication is ended. When the discrimination result in the step S24 is NO, an authentication error information is supplied to the terminal. When the discrimination result in the step S24 is YES, a step S25 develops the access qualification information of the user in accordance with the authentication information from the EEPROM 60 to the RAM 58.

A step S26 discriminates whether or not the user has a right to write information. When the discrimination result in the step S26 is NO, an access qualification error information is supplied to the terminal. But when the discrimination result in the step S26 is YES, a step S27 transfers the necessary information from the EEPROM 60 to the RAM 58 and a step S28 discriminates whether or not a designated write position exists. When the discrimination result in the step S28 is NO, a designation error information is supplied to the terminal. On the other hand, when the discrimination result in the step S28 is YES, a step S29 writes the data at the designated write position within the RAM 58. A step S30 develops the transaction serial number from the EEPROM 60 to the RAM 58, and a step S31 increments the transaction serial number in the RAM 58. The process then advances to a step S41 shown in FIG.6C.

In FIG.6C, the step S41 by calculation generates the verified data in conformance with a generating algorithm based on unique numbers such as the transaction serial number and the transaction date. A step S42 stores the verified data in the RAM 58. A step S43 discriminates whether or not all of the processes are correctly ended. When the discrimination result in the step S43 is NO, a write error information is supplied to the terminal. On the other hand, when the discrimination result in the step S43 is YES, a step S44 stores the write information, the verified data and the transaction serial number in the EEPROM 60. A step S45 discriminates whether or not the data are correctly stored in the EEPROM 60 in the step S44. When the discrimination result in the step S45 is NO, a memory error information is supplied to the terminal. When the discrimination result in the step S45 is YES, a step S46 assembles the transmitting data and an end information including a normal end information and the verified data is supplied to the terminal. When a transaction end information is received from the terminal, a step S47 ends the process by releasing the RAM 58 and the process is ended.

FIG.7 generally shows an embodiment of a card reader/writer which is used in the second embodiment. Of course a similar card reader/writer may be used in the first embodiment. In FIG.7, a card reader/writer 70 generally comprises a card inserting opening 71, a magnetic head 72, a timing belt 73, a card transport path 74, a contact part 75, a motor 76, a roller 77, a printed circuit 78 which has the CPU 54, the ROM 59 and the like arranged thereon, and a cover 79 which is indicated by a phantom line.

When the IC card 51 is inserted into the card inserting opening 71, the IC card 51 is transported along the card transport path 74 by a transport mechanism to a loaded position where contacts of the contact part 75 make contact with the corresponding terminals of the terminal group 52 of the IC card 51. The transport mechanism includes the motor 76 which rotates the roller 77 so as to drive the timing belt 73.

In this embodiment, the magnetic head 72 is provided to read a magnetic stripe of the IC card 51. The provision of the magnetic head 72 enables the card reader/writer 70 to read the magnetic stripes of both the IC card 51 and the conventional magnetic. In other words, there is card interchangeability among the IC cards and the magnetic stripe cards. However, it is not essential to provide the magnetic head 72 on the card reader/writer 70. In addition, the card reader/writer 70 may be a part of the terminal or be a unit independent of the terminal.

Further, the present invention is not limited to

nal means (9, 20) and corresponds to a selected service differs from an authenticate code stored in said second memory means (3, 4, 31, 32, 58, 59, 60) a predetermined number of times, said first lock flag which is set indicating that the selected service is non-accessible.

15. The transaction authentication system as claimed in claim 14, characterized in that said lock flag is set independently for each service.

16. The transaction authentication system as claimed in any of claims 1 to 15, characterized in that said second processing means (30, 54) comprises write means (5) for writing the transaction data which is received from said terminal means (9, 20) into the designated storage region of said second memory means (3, 4, 31, 32, 58, 59, 60), renewing means (7) for renewing a transaction execution identifying information which is stored in said second memory means every time the transaction data is received from said terminal means, and verified data generating means (6) for generating the verified data based on the transaction execution identifying information read from said second memory means.

17. The transaction authentication system as claimed in claim 16, characterized in that said verified data generating means (6) supplies the transaction execution identifying information which is read from said second memory means (3, 4, 31, 32, 58, 59, 60) as it is to said terminal means (9, 20) as the verified data.

18. The transaction authentication system as claimed in any of claims 1 to 17, characterized in that said second memory means (3, 4, 31, 32, 58, 59, 60) stores a card identification information, said second processing means (30, 54) of said integrated circuit card (1, 21, 51) supplies the card identification which is read from said second memory means together with the verified data, and said first processing means (10, 11) of said terminal means (9, 20) generates the transaction historical information which also includes the card identification information.

FIG.2

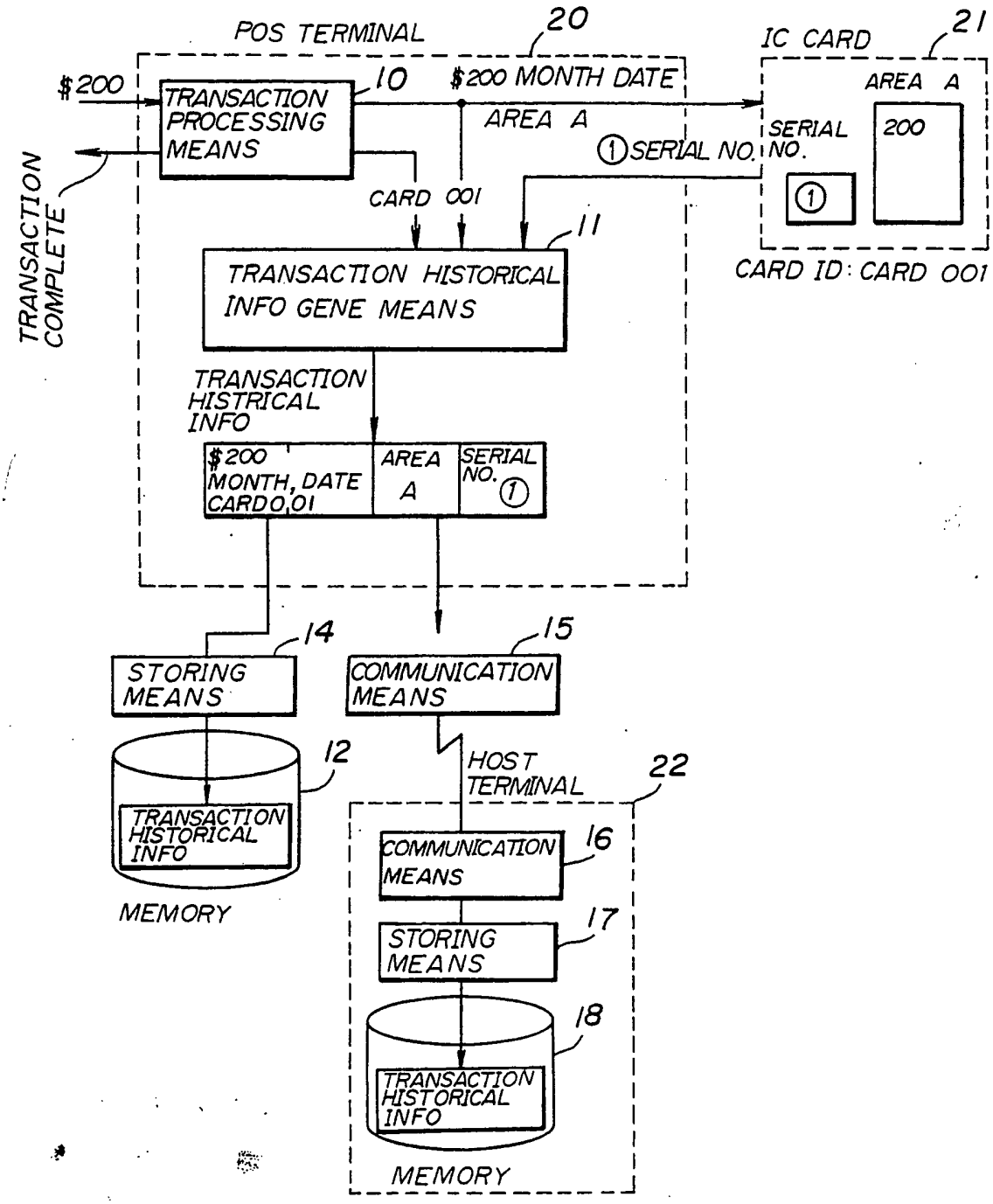


FIG. 4A

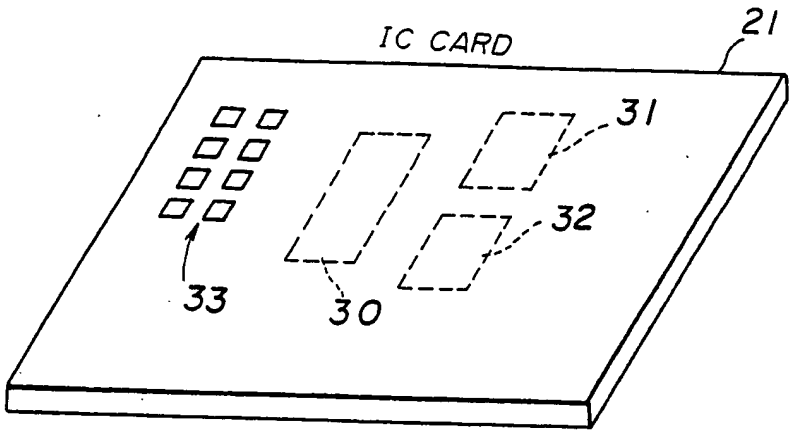

IC CARD
21
31
32
33
30

FIG. 4B

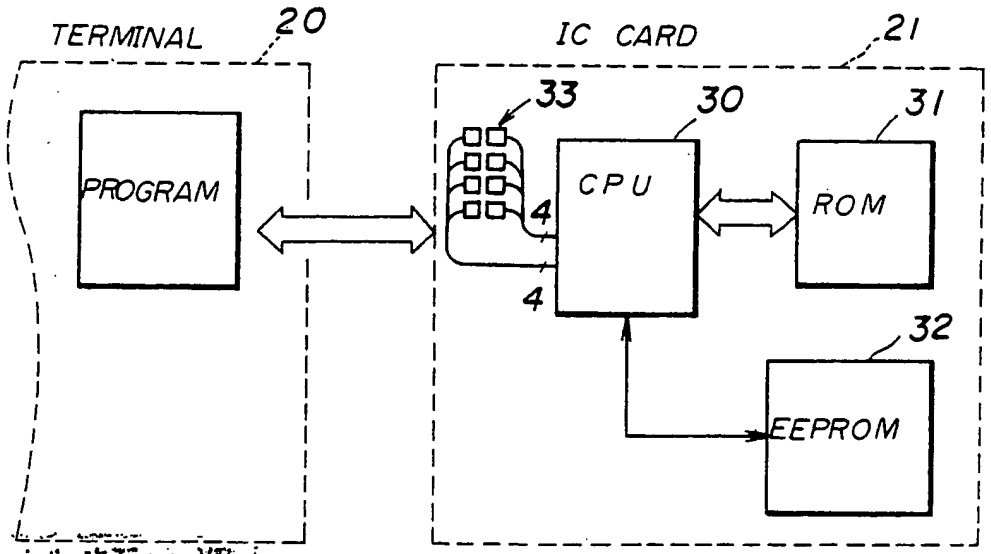

TERMINAL
20
PROGRAM
IC CARD
21
33
30
31
CPU
ROM
4
4
32
EEPROM

FIG.6A

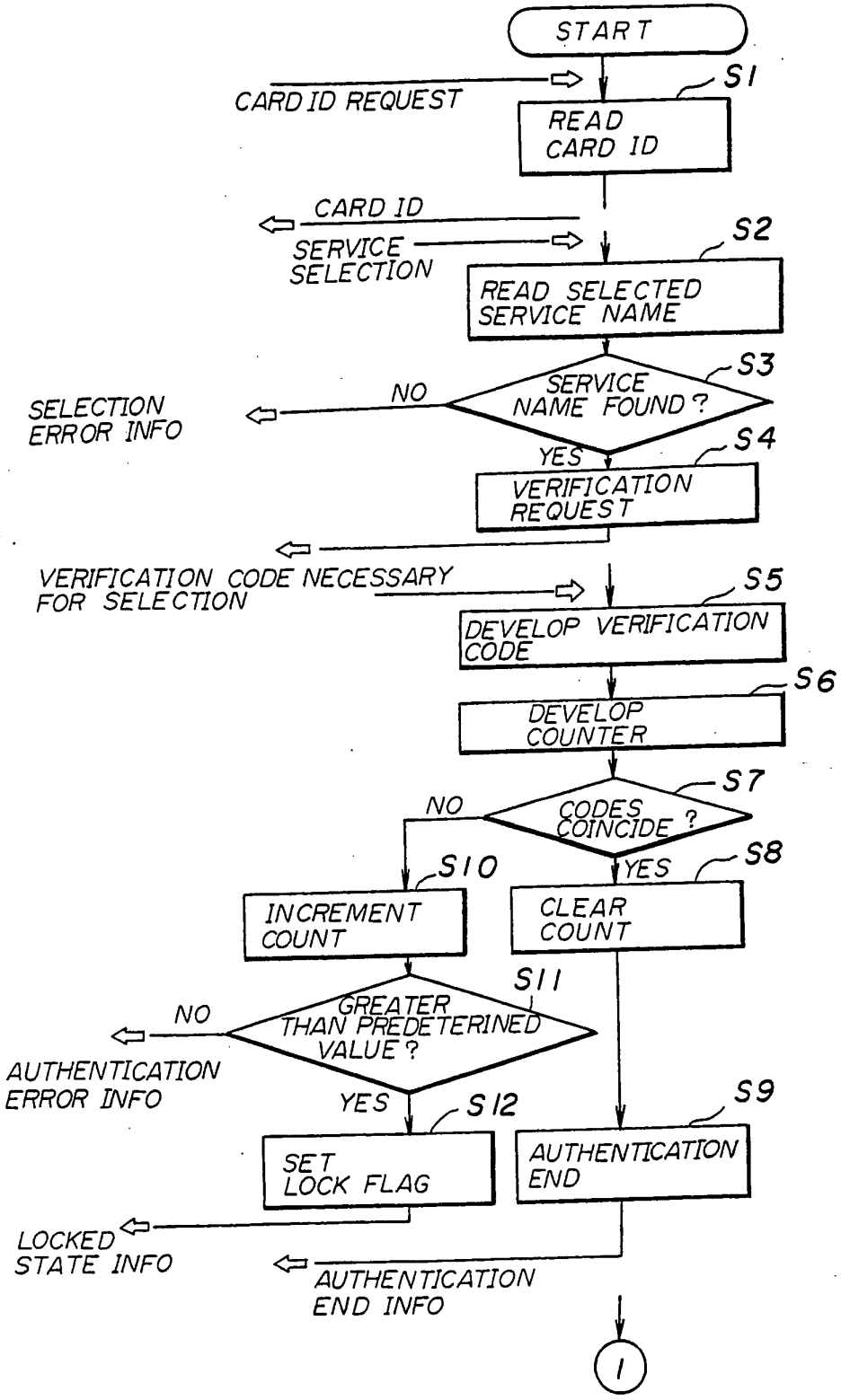
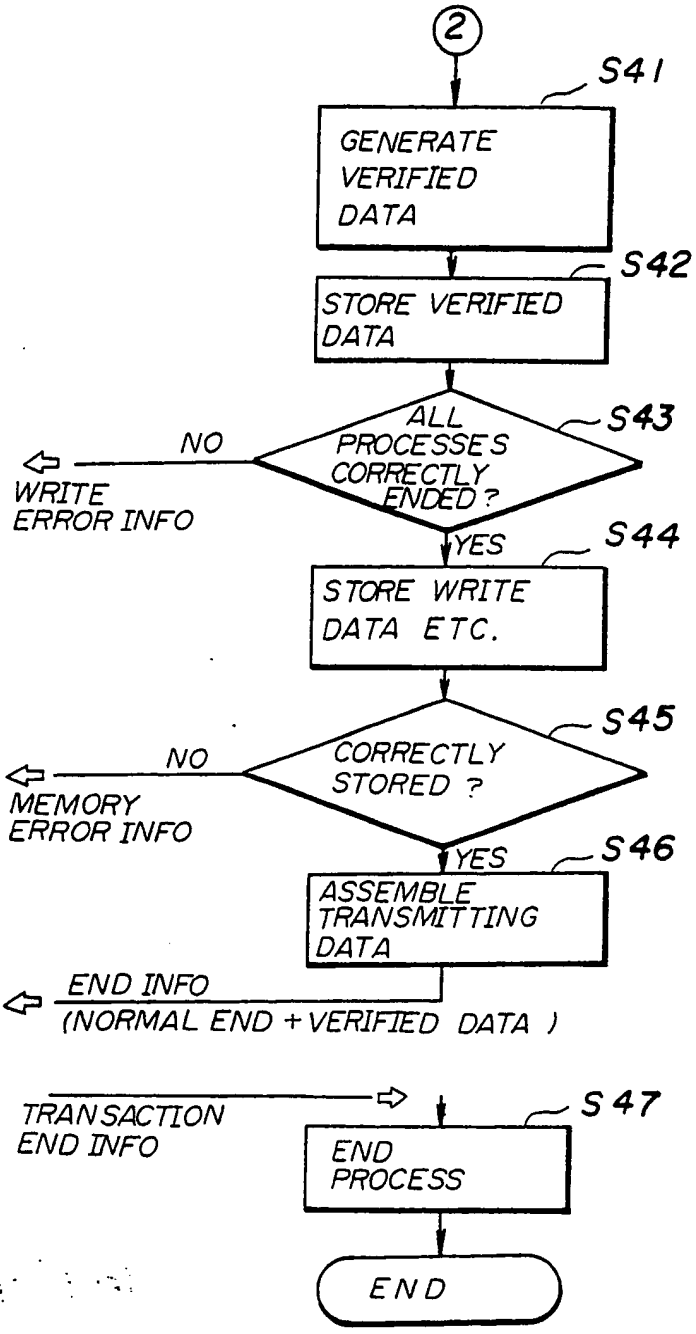

START
CARD ID REQUEST
S1
READ CARD ID
CARD ID
SERVICE SELECTION
S2
READ SELECTED SERVICE NAME
S3
SERVICE NAME FOUND ?
NO
SELECTION ERROR INFO
YES
S4
VERIFICATION REQUEST
VERIFICATION CODE NECESSARY FOR SELECTION
S5
DEVELOP VERIFICATION CODE
S6
DEVELOP COUNTER
S7
CODES COINCIDE ?
NO
YES
S8
S10
INCREMENT COUNT
CLEAR COUNT
S11
GREATER THAN PREDETERINED VALUE ?
NO
AUTHENTICATION ERROR INFO
YES
S12
SET LOCK FLAG
S9
AUTHENTICATION END
LOCKED STATE INFO
AUTHENTICATION END INFO
1

FIG. 6C


2
S41
GENERATE VERIFIED DATA
S42
STORE VERIFIED DATA
S43
ALL PROCESSES CORRECTLY ENDED ?
NO
WRITE ERROR INFO
YES
S44
STORE WRITE DATA ETC.
S45
CORRECTLY STORED ?
NO
MEMORY ERROR INFO
YES
S46
ASSEMBLE TRANSMITTING DATA
END INFO
(NORMAL END + VERIFIED DATA )
TRANSACTION END INFO
S47
END PROCESS
END

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Publication number: **0 363 122 A3**

# (12) EUROPEAN PATENT APPLICATION

(21) Application number: **89310051.1**

(51) Int. Cl.5: **G07F 7/10**

(22) Date of filing: **02.10.89**

(30) Priority: **03.10.88 JP 249561/88**

(43) Date of publication of application:
**11.04.90 Bulletin 90/15**

(84) Designated Contracting States:
**DE FR GB**

(88) Date of deferred publication of the search report:
**31.10.90 Bulletin 90/44**

(71) Applicant: **FUJITSU LIMITED**
**1015, Kamikodanaka Nakahara-ku**
**Kawasaki-shi Kanagawa 211(JP)**

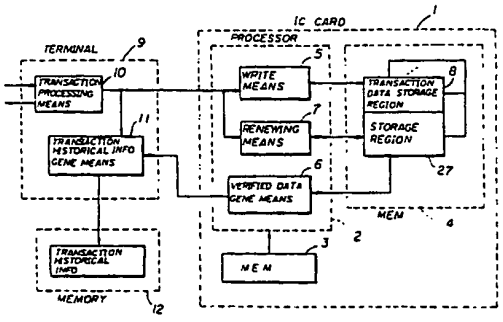
(72) Inventor: **Ogasawara, Nobuo**
**3-35-21-201, Nukuikitamachi**
**Koganei-shi Tokyo, 184(JP)**
Inventor: **Ozaki, Yoshiyuki**
**3-34-9, Nokendai Kanazawa-ku**
**Yokohama-shi Kanagawa, 236(JP)**

(74) Representative: **Stebbing, Timothy Charles et al**
**Haseltine Lake & Co. Hazlitt House 28**
**Southampton Buildings Chancery Lane**
**London WC2A 1AT(GB)**

## (54) Transaction authentication system.

(57) A transaction authentication system comprises a terminal (9, 20), a first memory (12, 18) and an IC card (1, 21, 51) which is detachably loaded into the terminal. The terminal supplies at least a transaction data which is related to a transaction and a designated storage region in a second memory (3, 4, 31, 32, 58, 59, 60) for storing the transaction data to the IC card when the IC card makes an access to a service via the terminal. A second processor (30, 54) of the IC card writes the transaction data received from the terminal in the designated storage region of the second memory and generates a verified data which is renewed every time the transaction data is written into the second memory. The verified data has a value in conformance with a predetermined generating algorithm and is stored in the second memory and also supplied to the terminal. A first processor (10, 11) of the terminal generates a transaction historical information which includes at least the designated storage region, the transaction data and the verified data and stores the transaction historical information in the first memory, so that a transaction is authenticatable from a correspondence of the verified data stored in the first memory and the verified data stored in the second memory.

FIG. 1




EP 0 363 122 A3